ボットによる不正メールの送信を防止するための検討

平田　祐二*，鈴木　秀和，渡邊　晃(名城大学)

Studies on the prevention method of wrong mail transmission caused by bot infection

Yuji Hirata, Hidekazu Suzuki, Akira Watanabe (Meijo University)

１．はじめに

インターネットの発展に伴い，ウイルスの被害が大きな問題となっている．近年ではボットと呼ばれる新しいタイプのウイルスが蔓延している．ボットとは悪性のプログラムであり，オープンソースとなっているため亜種が多く存在する．また感染前との差異を感じることなくコンピュータを使用できるので，感染したことに気づきにくいといった問題もある．

本稿では，ボットが組織化したボットネットからのスパムメール送信を防止するため，クライアント側でのスパムメール対策を検討した．

２．ボットネット

ボットに感染した PC が集まって構成されているネットワークのことをボットネットという．

攻撃者はIRC(Internet Relay Chat)サーバを通してボットに一斉に命令を送り，ボットをコントロールする．これらの命令により，ユーザの意思に関係なくクライアントから大量のスパムメールが送信される(Fig1.).

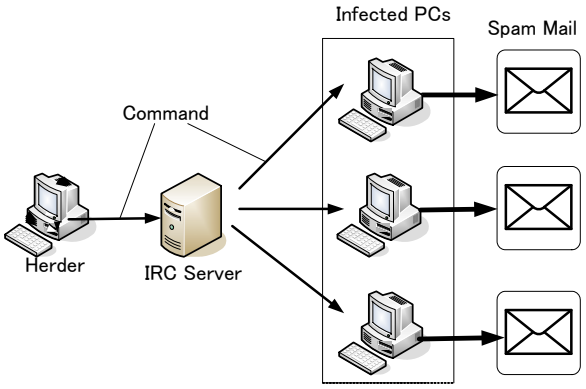


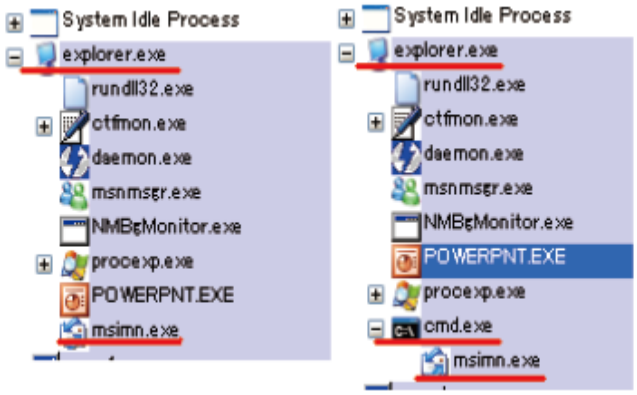
Fig1. ボットネットによるスパムメール送信

ボットネットによる被害を防止するには IRC サーバを停止する方法がある．しかし，IRC サーバを複数使用する場合や，IRC サーバを使用しないボットネットもあるため，ボットネット対策を IRC サーバや攻撃者(Herder)に対して施すことは難しいとされている．

３．クライアント側での対策

ボットは，攻撃者の命令を受けて初めて行動を起こすことに着目し，クライアント側でポート制御を行うことによりボットによるスパムメールを遮断する手法を検討した．

提案では，通常時は SMTP ポートを遮断しておく．このためにパーソナルファイアウォールのポート制御機能を利用する．この状態で MAPI(Messaging API)と呼ばれる，Windows 上で電子メールを扱うための関数群を監視する．メーラを呼び出したのが正常なユーザであると確認できた場合にのみ，ポートを開放し通信終了後にポートを再度遮断する．メーラを呼び出したのが正常なユーザかどうか判断するためにプロセスツリーを用いる．Fig2.で示すように MAPI が実行されたとき，正常時は explorer.exe が上位プロセスとなる．しかしボット感染時には、メーラの上位プロセスが cmd.exe となり正常時とは異なる．メーラの上位プロセスが explorer.exe と確認できた場合は正常と判断し，異なった場合はボットが実行したとみなしユーザにアラームをあげる．この方法により不正なメール送信を確実に防止する．



(1) 正常時　　(2) ボット感染時

Fig2.プロセスツリーによる上位プロセスの確認

４．むすび

ボットにより PC がスパムメール送信することを防止するための対策として，プロセスツリーを監視し，メールを送信したのが正しいユーザと判断できた場合にのみ，パーソナルファイアウォールの SMTP ポートを開放する手法を検討した．今後はこの手法の有効性を確認する．

文　献

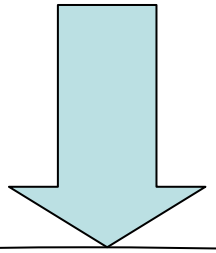
(1)　間宮　領一，渡邊　晃：不正メールの送信防止とボット感染検知の検討

ボットによる不正メールの送信を防止するための検討

名城大学理工学部
平田　祐二　鈴木　秀和　渡邊　晃

研究背景

- ウイルスによる被害の深刻化
- 様々なソフトウェアの脆弱性
- 自分は安全だと対策を怠るユーザ
- ボットネットによる大規模な攻撃

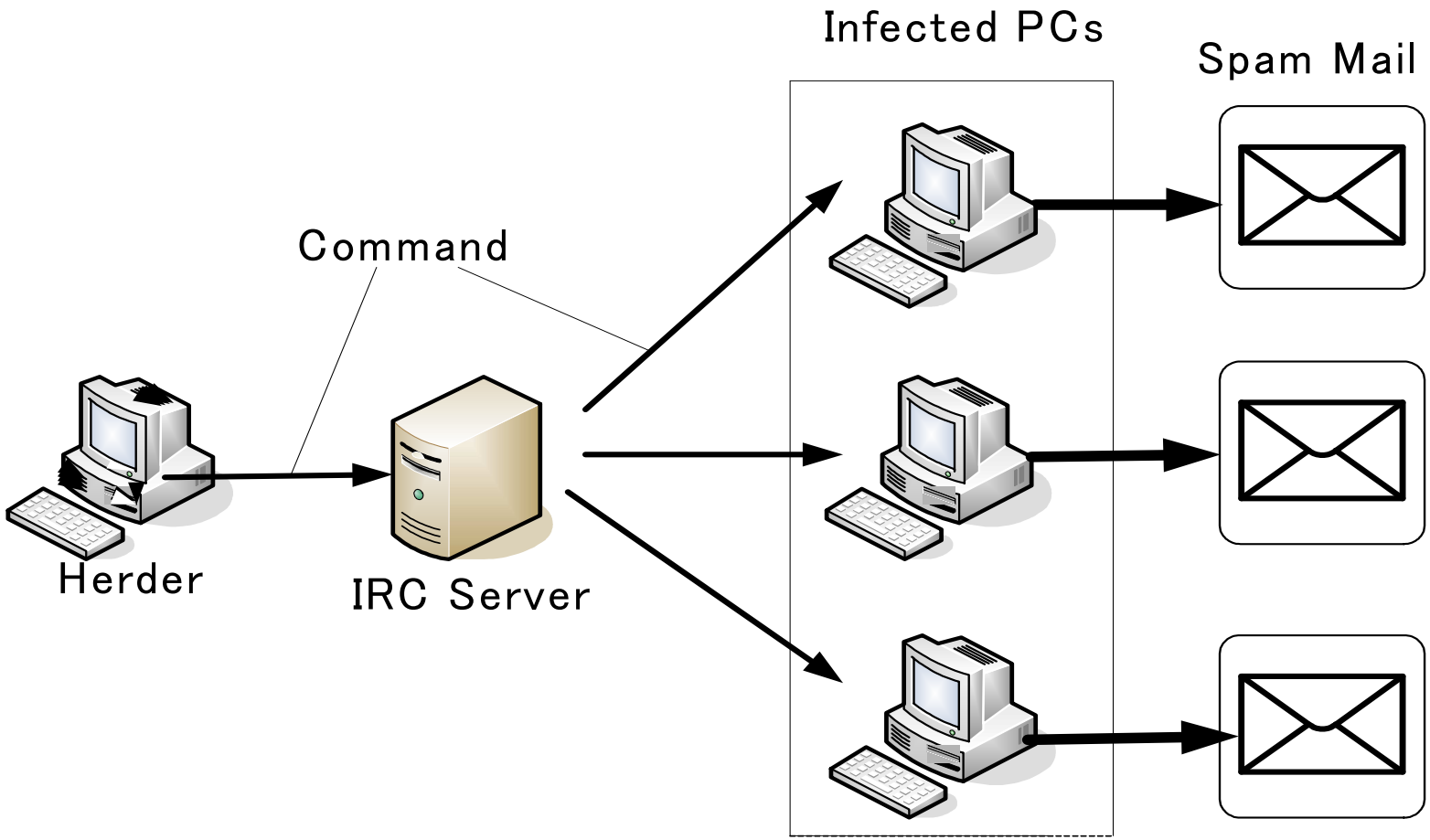


DoS攻撃、スパムメールの大量発生、個人情報流出

ボットとは

- ボット
  - 外部からコントロール可能な感染PC
  - 用途に合わせ様々な機能に拡張
  - 愉快犯から犯罪目的
  - 感染したことに気づきにくい
- ボットネット
  - ボットに感染したPCが集まって構成されているネットワーク
  - 数千～数万台で構成

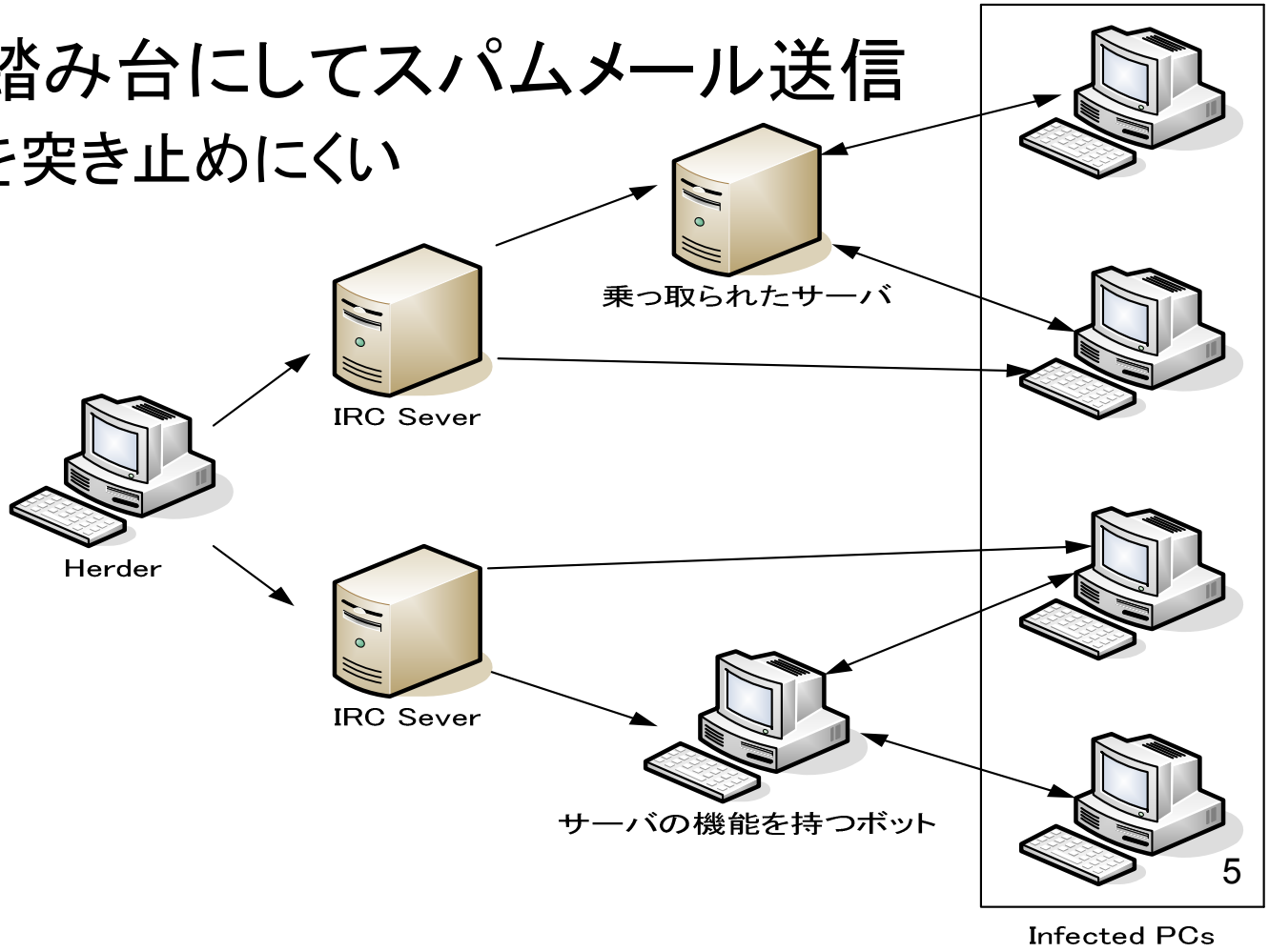
ボットネットによるスパムメール送信



IRC; Internet Relay Chat

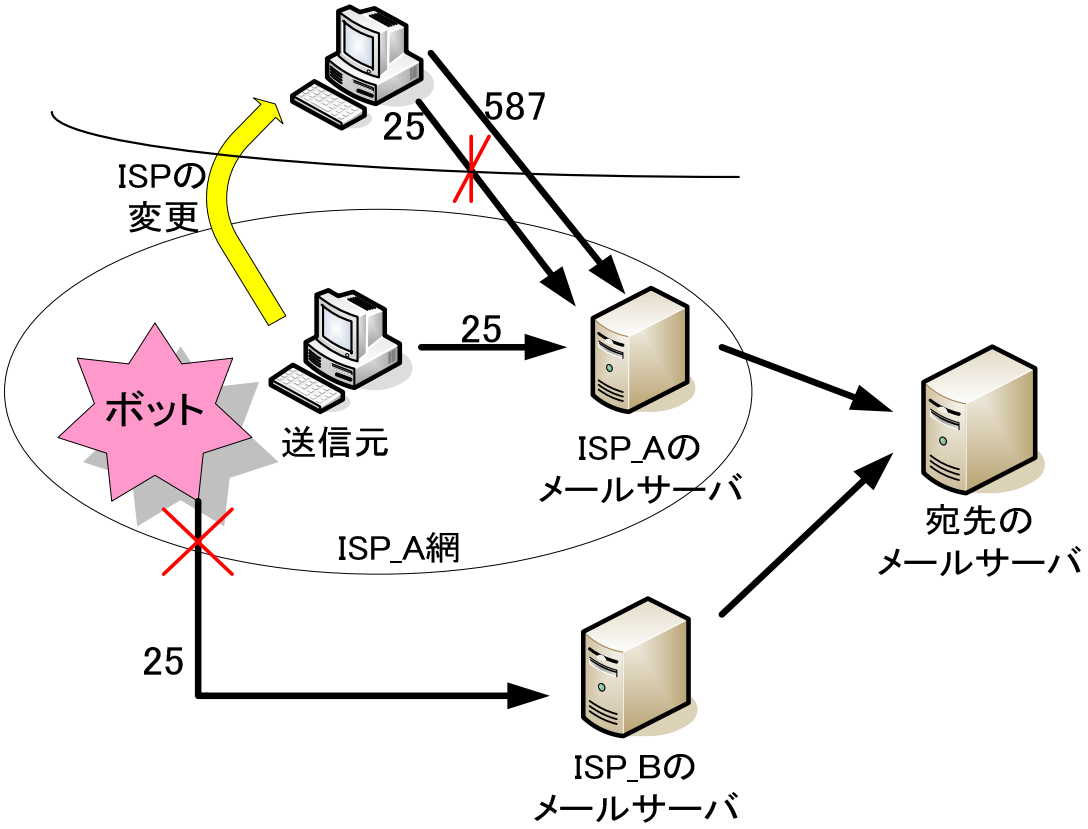
ボットネットを根絶することはほぼ不可能

- IRC Serverの冗長化
- サーバを踏み台にしてスパムメール送信
  - Herderを突き止めにくい



既存技術による対策

- アンチウィルスソフト
  - クライアントで実施
  - パターンマッチング方式によりボットを取り除く
- OP25B(Outbound Port25 Blocking)
  - プロバイダで実施
  - 契約外ISPのメールサーバを使用したSMTP通信を拒否
  - ユーザ認証機能付きのSMTP通信サービス



既存技術の問題

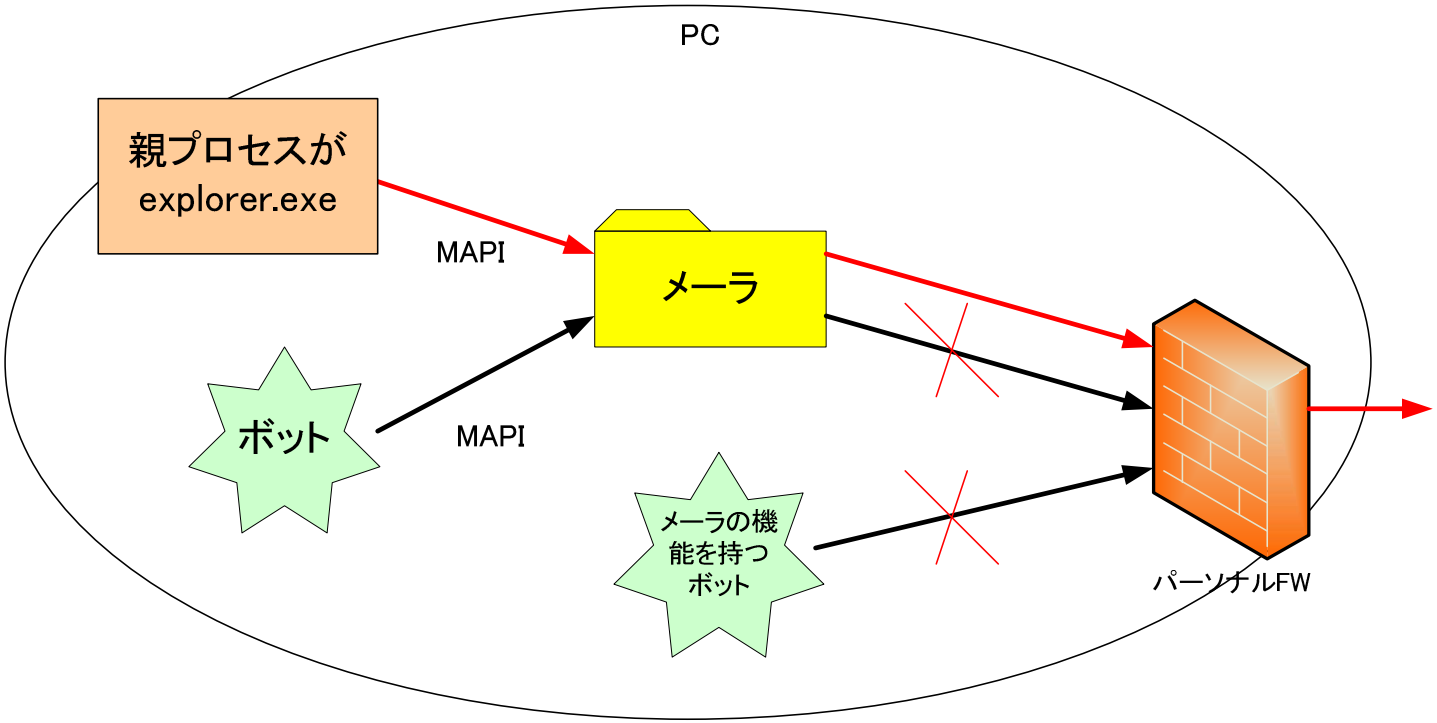
- アンチウイルスソフト
  - 定義ファイルに情報のないボットに対応できない
  - 新種のボットが数多く出回っている（1日あたり約20種類）
- OP25B
  - 正規のユーザを装ってのメール送信
    - 情報収集機能をもつボットがパスワードなどを取得した場合
  - 外出先からメールを送信できない
    - 引越しなどでISPを変更したが，メールアドレスは以前のものを使い続けている場合

提案方式

- クライアント側での対策
  - ボットの感染は避けられない
  - 二次災害を防止する
- 提案内容
  - 常にSMTPポート25，587番を遮断
  - MAPI(Messaging API)を監視
  - メーラのプロセスツリーを監視

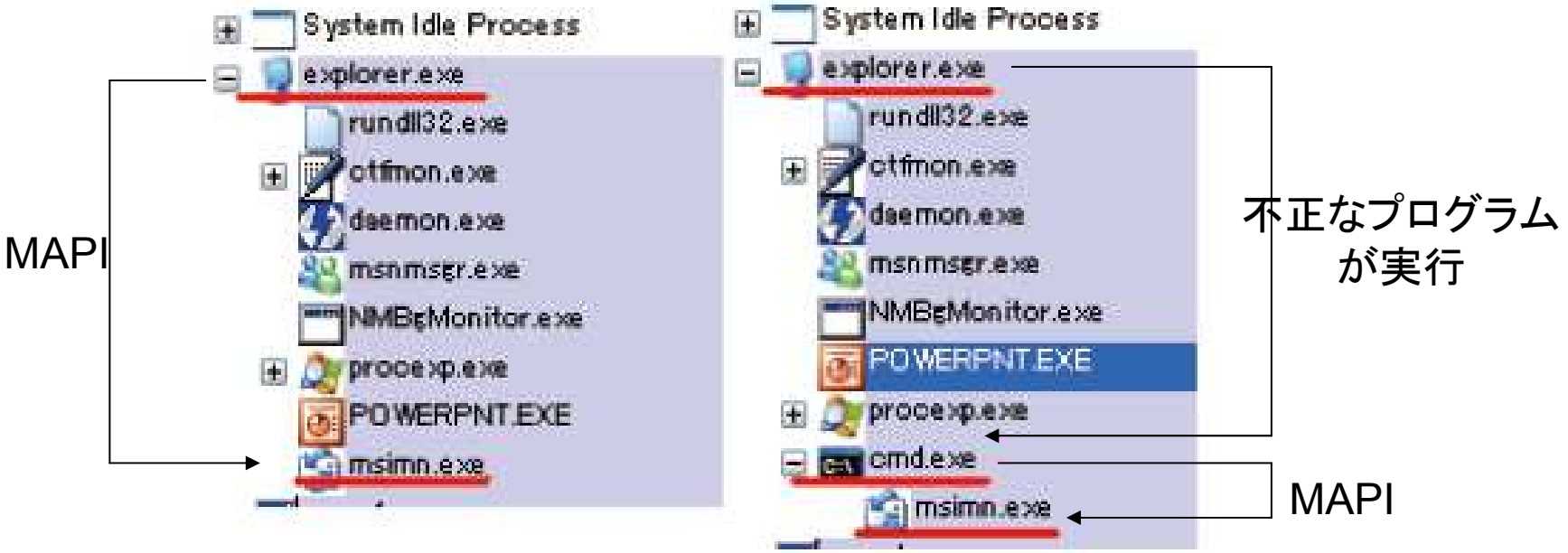
MAPIの監視

- MAPIとはWindows上で電子メールを扱うための関数郡で，一般的にWindowsではMAPIを用いてメールを送信する
- メーラを呼び出したのが正常なユーザと判断した場合
  →ポートを開放しメール送信を許可．送信終了後にポートを再度遮断
- 正常なユーザと判断するためにプロセスツリーを用いる



プロセスツリー

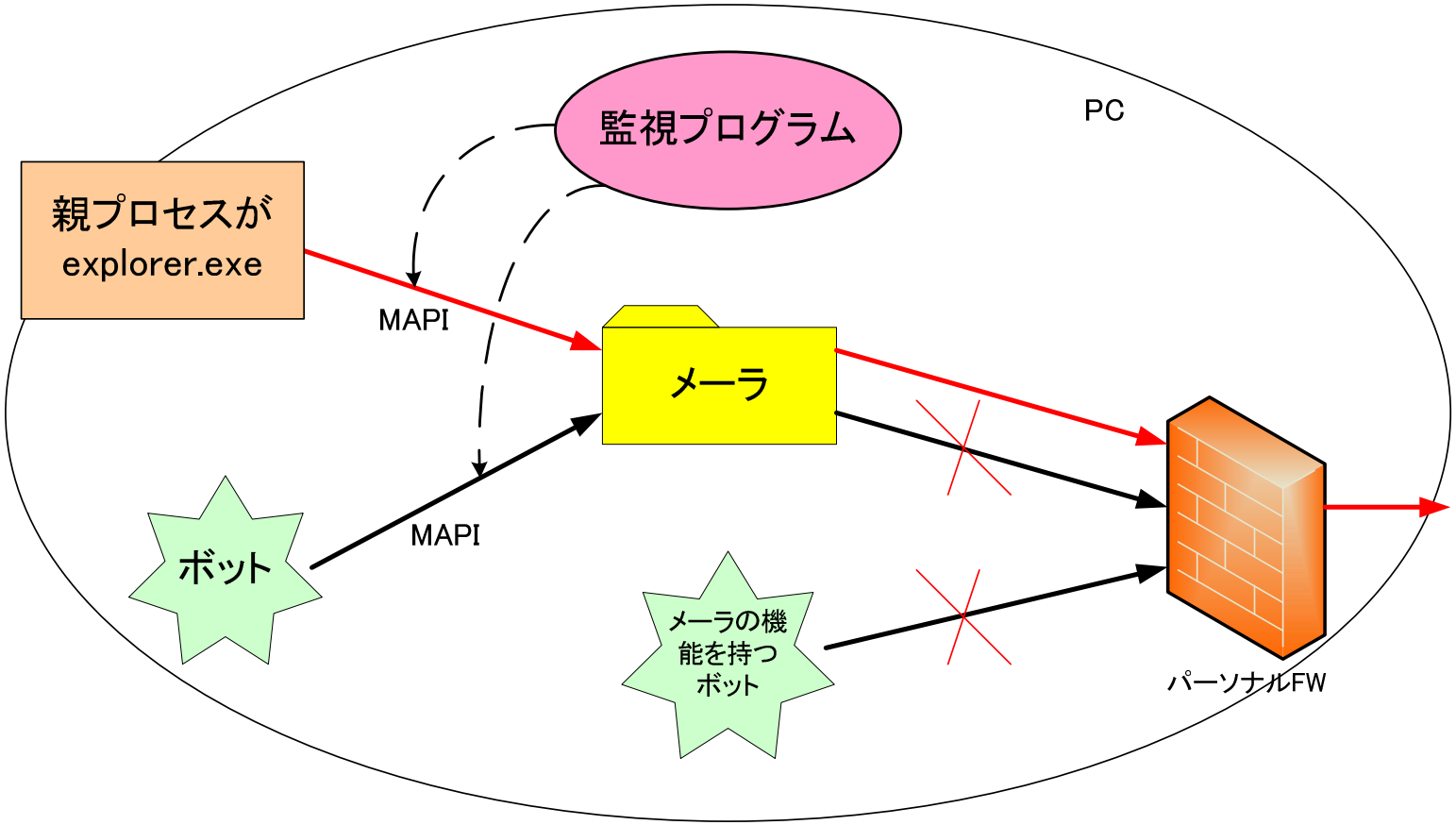
- 実行中のプロセスをツリー状に可視化したもの
  - 正常なメーラの親プロセスはexplorer.exe
- MAPIによるメーラ呼び出し時にメーラの親プロセスを確認
  - メーラの親プロセスがexplorer.exe
    →正常な実行と判断
  - メーラの親プロセスがexplorer.exe以外
    →不正なプログラムがメーラを呼び出したものと判断



1.正常時　　2.異常時

提案方式の動作

- 常にSMTPポート25,587番を遮断
- MAPIを監視しメーラの呼び出し元を確認
  - プロセスツリーを用いる
- メーラの親プロセスがexplorer.exeの場合にSMTPポートを開放（それ以外の場合は遮断したまま）



むすび

- スパムメール送信防止としてクライアントでの対策を検討
  - プロセスツリーを監視することにより通信を制御
- 今後の課題
  - 提案方式の実装と評価